DIGITAL CONTENT STORE SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to prior U.S. provisional application number 60/433,734, filed December 13, 2002, entitled *Music Net*, which is incorporated herein in its entirety by this reference made thereto.

FIELD OF THE INVENTION

[0002] The invention relates to the transfer, processing, sale, distribution, and usage of digital content in a network environment. More particularly, the invention relates to secure sale, distribution, and usage of digital content in a network environment.

BACKGROUND OF THE INVENTION

[0003] The Internet comprises a web of computers and networks, which are widely spread throughout the world. The Internet currently comprises millions of network connections, and is used by millions of people, such as for business, education, entertainment, and/or basic communication.

[0004] Digital content, such as sound recordings, *e.g.* songs, are often transferred across the Internet. In addition to the basic transfer of song files, numerous network enabled radio stations have been introduced, which provide content to listeners at computers across the Internet. Network enabled radio has significantly increased the magnitude and variety of content to recipients, as compared to conventional over-the-air radio broadcasts.

[0005] There are also several music stores on which are accessible across the Internet, by which songs and/or albums may be purchased, wherein digital content files are transferred to a user terminal upon purchase.

[0006] Several structures and methods have been described for the distribution of digital content in a network environment.

[0007] V. Shear, D. Van Wie, and R. Weber, *Systems and Methods for Matching, Selecting, Narrowcasting, and/or Classifying Based on Rights Management and/or Other Information*, U.S. Patent No. 6,112,181, 29 August 2000, describe that "[r]ights management information is used at least in part in a matching, narrowcasting, classifying and/or selecting process. A matching and classification utility system comprising a kind of Commerce Utility System is used to perform the matching, narrowcasting, classifying and/or selecting. The matching and classification utility system may match, narrowcast, classify and/or select people and/or things, non-limiting examples of which include software objects. The Matching and Classification Utility system may use any pre-existing classification schemes, including at least some rights management information and/or other qualitative and/or parameter data indicating and/or defining classes, classification systems, class hierarchies, category schemes, class assignments, category assignments, and/or class membership. The Matching and Classification Utility may also use at least some rights management information together with any artificial intelligence, expert system, statistical, computational, manual, or any other means to define new classes, class hierarchies, classification systems, category schemes, and/or assign persons, things, and/or groups of persons and/or things to at least one class."

[0008] T. Reussner and M. Britting, *Multi-Channel Device Having Storage Modules in a Loop Configuration with Main Control Unit for Controlling Data Rates and Modifying Data Selectively and Independently Therein*, U.S. Patent No. 5,517,672, 14 May 1996, describe "a multi-channel device for the digital recording and playback of audio signals, with a plurality of digital or analogue inputs and outputs and with one or more digital stores. For providing, with a not limited number of channels for recording and playback, possibilities for recording and playback over an unlimited period of time, with instantaneous access to any desired position of the recording, and carrying out overdubbing and editing without risk and freely selecting the time duration of the cross-fading, a bidirectional interface circuit with inputs and outputs is connected via a system-bus which conducts groups of parallel data, to one or more parallel connected storage modules, wherein a main control circuit driven by an operating unit is coupled to the system-bus and to the storage module or modules, and wherein each storage module

comprises at least one digital store, containing an exchangeable storage medium, and at least one digital buffer store such that the audio signals which are to be stored are kept available in the buffer store for their processing or during the exchange of the storage medium."

[0009] G. Lau, *Method and System for Subscription Digital Rights Management*, U.S. Patent Application Publication No. 20020198846, filed 6 June 2002, describes "[a] system and method for managing use of items having usage rights associated therewith. The system includes an activation device adapted to issue a software package having a public and private key pair, the public key being associated with a user, a license device adapted to issue a license, a usage device adapted to receive the software package, receive the license and allow the user to access the item in accordance with the license, and a subscription managing device adapted to maintain a subscription list including the public key associated with the user. License's is issued by the license device upon verifying presence of the public key in the subscription list corresponding to requested content."

[0010] T. Akashi, System for Delivering Music and Apparatus for Receiving Music Data, U.S. Patent Application 20020152878, filed Japan 23 April 2001, JP 2001-124342, filed U.S. 19 April 2002, Published 24 October 2002, describes a music data receiving apparatus, wherein "the music data receiver receives the music data broadcast by the broadcasting station, and then the reproducer reproduces the music data while the related information storage stores the related information for the music. The user, who is listening to the reproduced music, may give a download instruction, which orders to download the air, to the user's input receiver, if the user is pleased with the air. The download instruction is transmitted to the server accessor. The server accessor accesses the music delivery server, takes out the information for specifying the air to be downloaded from the related information storage, and then notifies it to the music delivery server. The music delivery server confirms the user or charges a fee executes, and then sends the specified air data."

[0011] D. Hughes, M. Carpenter, M. Massiha, and P. Nguyen, *Media Player for Distribution of Music Samples*, U.S. Patent Publication No. US 20020152876, filed 20

April 2001, published 24 October 2002, describe a "method and apparatus of music distribution from a media player. A media player is provided with a "send to friend" icon. In one embodiment, when the icon is selected, a clipping of the currently playing music selection is taken from a predetermined location in the music selection and compressed using a fidelity reducing compression technique to produce a sample of the current selection suitable for distribution. The compressed clipping is sent to a selected recipient or recipients by email in the background while the music selection continues to play. The recipient(s) can be either a default recipient(s) or a recipient(s) selected from a list as in an address book application."

[0012] J. Dunn, P. Lee, E. Stern, and B. Willner, *Broadcast Data Radio System and Receiver Apparatus Therefore*, U.S. Patent No. 6,163,683, 19 December 2000, describe a "radio broadcasting system for a virtual radio program broadcasting station uses a divided regional approach to broadcast digital and analog signals over a large geographic region divided into multiple overlapping but separate areas constituting small portions of the region. The small areas are served by separate transmission sources/towers supplied from a common source central to the station. The system supports reuse of allocated transmission parameters within non-neighboring small areas in the region. The station is "virtual" because its central source need not be in any of the small areas, and because it uses different transmission parameters in neighboring small areas in a manner that previously would be used by plural different stations. System transmissions include information signals sent in both analog and digital forms. The analog signals representing audibly reproducible programs, and the digital signals include instructions for controlling operations of receiver devices operating in the region. The digital signals also may include audibly reproducible program matter and instructions for controlling insertion of that matter into a program stream defined by analog transmissions. These transmissions are particularly useful for varying tuning parameters of mobile receiver devices disclosed herein to automatically and seamlessly maintain the devices tuned to the respective virtual station throughout the region, while the devices are transported across virtual boundaries between the small areas within the region. The system enables the virtual station to alternately present audible matter of general interest

throughout the region and audible matter relevant exclusively to a small area within the region (e.g. advertisements specifying locations and services offered by commercial establishments within a respective area, and announcements specifying locations of public facilities such as libraries, hospitals, etc.). Transmitted digital information is retained in mass storage units associated with receiver devices and is used for adjusting tuning parameters as a device is transported across the small areas of the region, as well as for providing a portion of the program content that is played at the device during such movement."

[0013] M. Gell, M. Manning, and J.L. Martin, *System for Selective Communication Connection Based on Transaction Pricing Signals*, U.S. Patent No. 5,802,502, 01 September 1998, describe a "communications network in which user equipment is provided with a selecting device which communicates with a pricing device in service provider equipment. When communications or other services are required, the selection circuit polls a plurality of service providers, and the pricing circuit of each service provider generates a price signal indicating the level of price for its services. The selection circuit then selects a service provider, based on price (and also other factors such as quality of service)."

[0014] D. Stebbings and J. Kadin, *Method and Apparatus for High Speed Duplication of Audio or Digital Signals*, U.S. Patent No. 5,325,238, describe a "method of and apparatus for recording information from a master medium onto a slave medium. In one embodiment, digital information on a master medium is reproduced and stored at a first rate, typically at real time, in a first high speed digital storage device such as a magnetic disk drive. The digital information stored in the first storage device, when needed, is transferred at a second rate, much higher than the first, to a second digital storage device in which it is stored until it is scheduled for duplication, at which time the digital information is repeatedly played back at a third rate, much higher than the first rate and slower than the second rate, is converted from digital information into analog information and applied to a duplicating device for recording the analog information onto a slave medium. Because the information stored in the first digital storage device is not directly used in production, the duplicating device can be duplicating information

previously transferred from the first storage device to the second at the same time information is being reproduced from a master medium and loaded, in real time, into the first storage device."

[0015] D. Spencer, W. Lutton, M. Hsu, G. Anderson, D. McMahon, and A. Schaller, *Closed-Loop Delivery to Integrated Download Manager*;, U.S. Patent Application Publication No. US 20030014436, filed 27 June 2001, Publication 16 January 2003, describe "[m]ethods, apparatus and system, including computer program products, implementing and using techniques for delivery of media files to a particular digital media playback device. The system comprises a content server and a download manager located in the digital media playback device. The content server receives device-identifying information obtained from the digital media playback device, and distributes media files in response to the received device-identifying information. The download manager forwards device-identifying information to the content server over a public communication network and receives media files over the public communication network from the content server for playback on the particular digital media playback device."

[0016] Other structures and methods have been described for the distribution of content in a network environment, such as: *Method and System for Downloading Digital Music*, Taiwan Patent No. TW 497055; *Network-Based Published Works Reproduction System*, Japanese Patent No. JP 2003069768; *Digital Music Data Reproduction Device Consists of Decoding and Expanding Circuits Connected Through Internal Path of Computing Element*; Japanese Patent No. JP 2002108395; *Web-Based Protection and Secure Distribution for Digital Music*; International Conference on WEB delivering of 23-24 November 2001, Changseng Xu, Yongwei Zhu, and David Dagan Feng, Florence Italy; *IP Data Over Satellite to Cable Headends and a New Operation Model with Digital Store and Forward Multi-Media Systems*; Conference Paper.

[0017] An iTUNES ™ internet music store has been introduced by Apple Computer, Inc., of Cupertino, CA, as seen at http://www.apple.com/music/store/, which provides for the browsing and purchase of digital music files, which are associated with usage rights, such as for playing or burning onto media.

[0018] It would be advantageous to provide a digital content store system and an associated methodology which provides acquisition and distribution of secure digital content, *e.g.* such as but not limited to music, video, games and software, and controlled usage of the secure digital content. The development of such a digital music store system would constitute a major technological advance.

[0019] It would also be advantageous to provide a digital content store system over a network, and an associated methodology which provides secure content and controlled usage of the secure content, wherein the client machine is not required to be connected to the network during use of the content. The development of such a digital content store system would constitute a major technological advance.

[0020] Furthermore, it would be advantageous to provide a network-enabled digital content store system and an associated methodology which provides secure digital content and controlled usage of the secure digital content, wherein the digital rights management is provided within the client machine after the content is transferred to the client machine. The development of such a digital content store system would constitute a major technological advance.

SUMMARY OF THE INVENTION

[0021] The digital content store provides users with an opportunity to purchase authorized usage of digital content, such as single or multiple music tracks, video, movies, and/or video games. The users can also buy license to a desired track for a fixed number of times, *e.g.* preferably the users can listen on three different machines simultaneously. Users can also burn a play list of X number of times, for example ten. The burn limit preferably applies to the play list, not the song. Mixed media capability is provided that allows the purchase of digital content and/or physical media. The digital content store system comprises a unique digital rights management system and a back-end enabling system that controls these digital rights.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] Figure 1 is a schematic diagram of a digital music store system implemented between a client machine and a store server;

[0023] Figure 2 is a detailed schematic diagram of client and server side architecture within a digital music store system;

[0024] Figure 3 is a download flowchart for a digital music store system;

[0025] Figure 4 is a schematic diagram of security systems download and playback operations for a client machine adapted to access a digital music store;

[0026] Figure 5 is a schematic diagram of security systems download and burn operations for a client machine adapted to access a digital music store;

[0027] Figure 6 is a functional block diagram of a digital content player associated with a digital music store system;

[0028] Figure 7 is a schematic diagram of asset encryption and the establishment of an associated asset license;

[0029] Figure 8 is a functional block diagram of a draft data model within a digital music store system;

[0030] Figure 9 is a schematic diagram of physical content purchase and availability of streamed and/or downloadable content;

[0031] Figure 10 is a functional block diagram of a playlist;

[0032] Figure 11 is a schematic diagram of a transfer of an encrypted asset and prevention of asset use without associated license;

[0033] Figure 12 is a schematic diagram of a transfer of an encrypted asset and prevention of asset use without an authorized license;

[0034] Figure 13 is a schematic diagram of a transfer of an encrypted asset and a system prompt to establish authorized use for the asset;

[0035] Figure 14 is a schematic diagram of physical content purchase for an alternate recipient and availability of streamed and/or downloadable content;

[0036] Figure 15 is a functional block diagram of a basic digital music player; and

[0037] Figure 16 is functional block diagram of a digital music player comprising asset security.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0038] Figure 1 is a basic schematic diagram 10 of a digital content store system 12a implemented between a digital content store 14 and a client machine 16. A user USR at a client machine 16 typically accesses the digital content store 14 through a store link and account module 38, such as through a user interface 103 (FIG. 2).

[0039] The store module 38 is typically associated with a selectable inventory of assets 304 (FIG. 7), which are typically accessible 42,44, upon purchase or other redemption, as encrypted assets 18, *e.g.* 18a-18p, such as though a digital fulfillment center 40.

[0040] A user USR at a client machine 16 can selectably purchase encrypted assets 18, through the entry of purchase information 34, whereby the encrypted assets 18 are delivered, such as through streaming 48 and/or downloading 50, which may comprise a download prompt 52 and download delivery 54, wherein the download delivery 54 comprises both asset delivery 174 (FIG. 3) and license delivery 178 (FIG. 3) to the client 16.

[0041] In some system embodiments 12, the user USR may also purchase physical inventory of content 56, *e.g.* such as compact discs CDs and/or digital video disks DVDs, which are then shipped 58 to the intended user USR. Upon purchase 34, some system embodiments comprise both delivery of physical content 56, along with streaming 48 and/or downloading of encrypted digital content 18, whereby the intended user USR can quickly access content 18, such as songs, movies, games, or other content 18.

[0042] As seen in Figure 1, a license 20 for an encrypted asset 18 comprises an asset key 22 and usage rights 24 for the encrypted asset 18. Usage of the encrypted asset 18 typically comprises playing the asset 18 through an audio output 28, or writing, *i.e.* burning, the asset 18 to a media 32.

[0043] The license information 20 comprises the asset rights 20 for the encrypted content 18, and comprises both an asset key 22 and usage rights 24, which are retained within a secure key locker 26. Playback of an encrypted asset 18 requires that the asset

rights 20 are retrieved, *i.e.* extracted from the secure key locker 26, whereby the asset key 22 operates upon the asset 18, such as through decryption, decoding and/or rendering. The enabled asset is then played as desired by the user USR, in compliance with the usage rights 24. The asset key 22 is preferably bound to the client machine 16, such as through machine fingerprinting or in conjunction with the machine identification 21.

[0044] An authorized use of the encrypted asset 18 may comprise an authorized transfer 29 of the asset 18 to media or storage on a player 390 (FIG. 15), 400 (FIG. 16), *e.g.* an MP3 player, or to another machine 16, as allowed by usage rights 24. In conjunction with an authorized transfer 29, a modified license 20 is preferably included with the encrypted asset 18, such as comprising an asset key 22 which is unbound from the primary client machine 16, and a portion of appropriate usage rights 24, *e.g.* such as for authorizing play of a media 56.

[0045] Figure 2 is a detailed schematic diagram of client and server side architecture within a digital content store system 12b. Client software 84 provides communication functionality to server 14, and to a digital content player 86, *e.g.* a media player 86. A media database 82 stores assets, such as acquired encrypted assets 18, and may preferably be used to store other assets, such as unencrypted assets 306 (FIG. 7) and/or associated metadata 306 (FIG. 7).

[0046] The client software 84 typically comprises a download module 92, a license download module 94, and may also comprise other functionality, such as stored user interface pages 90 and/or promotional links 88, *e.g.* for a digital content store 14.

[0047] The digital content player 86 typically comprises a secure digital content/music store (DMS) content handler 96, digital rights management (DRM) 98, AOL Comm 100, and secure AAC 102.

[0048] On the server side 14, promotional links and user account 38 typically comprises a user interface 103, download and order history 46, content download 104, license download 106, and license purchase 108. An encrypted content store 110 stores encrypted content 18, such as is available for purchase within the digital content store system 12. Other server storage comprises content metadata and usage rights 112, keys database 114, and a user database 116.

[0049] As seen in Figure 2, raw content 122, such as from labels 124, is sent to content acquisition 118, wherein the incoming raw content 122, comprising raw assets 304 (FIG. 7) and associated metadata 306 (FIG. 7), is processed, within an encoding and encryption module 120.

[0050] The back office support system 108 shown in Figure 2 comprises pricing 142, a user database 144, royalty processing 130, member services 132, billing and micropayments 136, taxation 138, order management 140, and jax/fraud 134. Pricing/SKU information 126 is typically sent to the back office support system 108, such as from metadata 306 received at content acquisition 118. As well, royalty reporting or other output information 128 is typically sent from the back office support system 108 to the labels 124.

[0051] As seen in Figure 2, content and associated license information is sent from the server 14 to the client machine 16, through the client software 84. Encrypted content 18 is transferred to the media database 82, where it is retrievable for usage through the digital content player 86. As needed, the digital content player 86 may interact through the client software 84, such as to communicate with the server 14, *e.g.* to update usage information, or to prompt the user USR to acquire or extend asset rights 20.

Playback of Acquired Assets.

[0052] During playback, the digital content player playback engine 250 (FIG. 6), which is preferably secure and tamper resistant (*e.g.* such as provided by SAFEWRAP™, by Macrovision, Inc., of Santa Clara, CA, extracts the asset key 22 from the secure key locker 26, and then decrypts, decodes, and renders the asset 18. The media pipeline is protected up until the handoff to the sound card 28 (FIG. 1). In preferred embodiments of the digital music store system 12, users USR do not need to be online in order to listen to their music 18.

[0053] If the digital content player 86 detects that the key 22 is missing, or is not valid for the machine 16 in question, the digital content player 86 preferably first plays a sample of the song 18, *e.g.* such as a 30 second clip, and then the digital content player 86 presents the user USR with a purchase opportunity. If the user USR chooses to

purchase 34, they are taken to the digital music store 14 to complete the process 34. The entire key mechanism is preferably seamless to the user experience.

Acquisition of Assets and Usage Rights.

[0054] Figure 3 is a flowchart 160 showing asset purchase and download within a digital content store system 12. At a purchase step 166, user USR at a client machine 16 purchases content 18, *e.g.* a song, from a digital store 14, such as through a store server 164. Upon a successful purchase transaction 166, a ticket 165, *e.g.* such as a desTicket 165, is sent 168 to the user terminal 16, typically from the store server 164.

[0055] The ticket 165 shown in Figure 3 is preferably a file that comprises a proprietary mime format. The ticket 165 launches the download manager (DM) 162 within the client terminal 16. The download manager 162 brokers transactions between the client machine 16 and the fulfillment server 40.

[0056] In some system applications, a browser 84 within the client machine 16 is used to send purchase information 166 and receive the ticket 165. For example, the browser 84 may be internet browser software 84, or proprietary client software 84, *e.g.* AOL CLIENT™ software 84, available through America Online Inc. (AOL), of Dulles, VA, which acts as an embedded browser 84, such as within INTERNET EXPLORER™, available through Microsoft, Inc., of Redmond, WA.

[0057] At step 170 shown in Figure 3, the browser 84 receives the ticket 165, and passes a request to play the ticket, *e.g.* "application/desTicket" to the operating system 260 (FIG. 6), *e.g.* Windows. The operating system 260 typically associates "application/desTicket" 165 with a .dmt file extension, and associates .dmt to a filetype DMTFile. The operating system 260 then launches the download manager 162 application, which is associated with the DMTFile.

[0058] The download manager 162 requests 172 the asset 18 from the content fulfillment server 40, such as over an established http connection 173. The asset 18 is sent or streamed 174 down to the client 16, in response to the request 172.

[0059] The download manager 162 also requests 176 a license 20 corresponding to the asset 18 from the fulfillment server 40, and sends 180 machine characteristics 21, *e.g.*

machine identification, to the server 40. In preferred embodiments of the digital content store system 12, the machine identification comprises machine fingerprinting, available through AMToolkit™, by TryMedia Systems, Inc, of San Francisco, CA.

[0060] In response to a proper license request 176, the fulfillment server 40 sends or streams 178 the license 20 to the client 16. The license 20 comprises both an asset key 22 and usage rights 24 for the asset 18. The request 176 for the license 20, the transmission 180 of machine characteristics 21 to the server 40, and the transmission 178 of the license 20 from the server 40, are preferably performed over a secure connection 181, *e.g.* https, established between the client machine 16 and the server 40. In some system embodiments, the secure session 181 comprises an authenticated session 181. In alternate system embodiments 12, the secure session 181 is initiated through a one-time, *i.e.* single use, ticket.

[0061] The download manager 162 binds the received license 20 to the client machine 16, and stores the asset key 22 in the secure key locker 26 (FIG. 1). In some system embodiments, the binding to a client machine 16 comprises a machine fingerprinting feature of AMToolkit™, available through TryMedia Systems, Inc., of San Francisco, CA.

[0062] The download manager 162 also sends an acknowledgement 182 to the content fulfillment server 40, wherein the acknowledgement 182 comprises the receipt of the asset 18 and the license 20.

[0063] In some system embodiments, the download manager 162 comprises a portion of digital content player software 86, *e.g.* such as a subset of AOL MediaPlayer 244 (FIG. 6), available through America Online Inc. (AOL). The download manager 162 shown in Figure 3 is preferably a tamper-resistant application, *e.g.* such as provided by SAFEWRAP™, by Macrovision, Inc., in which unauthorized use, such as within the client machine 16, or between a client machine 16 and a content fulfillment server 40, is minimized or eliminated. Some embodiments of the download manager 162 also comprise one or more additional layers of license encryption.

[0064] Figure 4 is a schematic diagram 200a of download 54 and playback 27 security systems within a client machine 16 adapted to access a digital content store 14.

Figure 5 is a schematic diagram 200b of download 54 and burn 29 security systems within a client machine 16 adapted to access a digital content store 14.

[0065] As seen in Figure 4 and Figure 5, a client machine 16 typically comprises a digital content player 86, a download manager 162, an input module 205, an output module 211, an asset rights module 207, and a secure key locker 26. Some system actions between modules are preferably performed over secure access channels 230.

[0066] The input module 205 is preferably tamper resistant, such as provided by SAFEWRAP™, and provides encryption of asset keys 22, and encryption of usage rights 24.

[0067] The output module 211 is also preferably tamper resistant, and performs decryption of usage rights 24, determination of sufficient usage rights for assets 18, decryption of asset keys 22, and upon a proper request, decryption of encrypted assets 18 with the associated asset key 22. As well, if usage rights are to be affected by any action or use, the output module 211follows the required steps for updating the asset rights into the secure key locker 26.

[0068] The asset rights module 207, which is preferably tamper resistant and uniquely linked to a client machine 16, such as through machine fingerprinting, provides a variety of secure functions, such as for downloading operations between the input module 205 and the secure key locker 26, or for playback or burn functions between the secure key locker 26 and the output module 211.

[0069] For example, the asset rights module 207 binds encrypted asset keys 22 to the client machine 16, combines machine-bound encrypted asset keys 22 and encrypted user rights 24 into asset rights, *i.e.* licenses 20, stores asset rights 20 within the secure key locker 26, retrieves the asset rights 20 as needed from the secure key locker 26, breaks asset rights 20 into asset keys 22 and usage rights 24, and unbinds asset keys as needed from the client machine 16.

Downloading Op rations.

[0070] As seen in Figure 4 and Figure 5, the client machine 16 provides secure downloading on of encrypted assets 18 and licenses 20. Once an encrypted asset 18 is

streamed or downloaded 174 (FIG. 3) to the download manager 162 at the client machine 16, the download manager stores 204 the encrypted asset 18 to a specified location, such as within the media database 82 (FIG. 2). The download manager 162 also transfers the downloaded 178 asset rights 20 to the input module 205, such as over a secure access channel 230, wherein the asset rights 20 comprise the associated asset key 22 and usage rights 24.

[0071] Upon encryption of the asset key 22 and usage rights 24, the input module 205 sends 208 the encrypted asset key 22 and encrypted usage rights 24 to the asset rights module 207, such as over a secure access channel 230. The asset rights module 207 binds 217 the encrypted asset key 22 to the client machine 16, combines the machine-bound encrypted asset key 22 and encrypted user rights 24 into machine bound asset rights 20, and stores 210 the machine-bound asset rights 20 within the secure key locker 26, typically over a secure access channel 230.

Playback Operations.

[0072] As seen in Figure 4, the client machine 16 provides playback 27 of encrypted assets 18 associated with asset rights 20. Upon a user request 209 for a playback 27 of an encrypted asset 18, the digital content player 86 sends 212a a request to the output module 211, which in turn sends a corresponding request 214a to the asset rights module 207, such as over a secure access channel 230, to get the encrypted asset key 22 and encrypted usage rights 24 associated with the encrypted asset 18.

[0073] The asset rights module 207 sends a request 216a to the secure key locker 26, such as over a secure access channel 230, to get the machine-bound asset rights 234. In return, the machine-bound asset rights 234 which correspond to the encrypted asset 18 are sent 218a from the secure key locker 26 to the asset rights module 207, preferably over a secure access channel 230. The asset rights module 207 breaks 219 the machine-bound asset rights 234 into the encrypted asset key 22 and encrypted usage rights 24, and sends 220a the encrypted asset key 22 and encrypted usage rights 24 to the output module 211, preferably over a secure access channel 230.

[0074] The output module 211 decrypts the usage rights 24, and confirms that the playback 27 is allowed by the usage rights 24. If playback 27 is allowed, the output module decrypts the asset key 22 that is associated with the encrypted asset 18, and decrypts the encrypted asset 18 with the asset key, to serve 224a the playback request 212a.

[0075] If playback 27 is not allowed, the output module 211 typically prevents decryption and full playback 27 of the asset 18. In some preferred embodiments, the output module 211 may proceed to authorize the playback 27 of a portion or sample of the asset 18, which may be accompanied with a prompt or link to obtain asset rights 20 for the encrypted asset 18.

[0076] If usage rights are affected by playback, the output module 211 initiates the required steps to update asset rights 20 into the secure key locker 26. For example, the output module may update and encrypt the asset key 22 and usage rights 24, and send 222a the encrypted updated asset key 22 and usage rights 24 to the asset rights module 207, preferably over a secure access channel 230. The asset rights module 207 binds 217 the encrypted updated asset key 22 to the client machine 16, combines the machine-bound encrypted updated asset key 22 and encrypted updated user rights 24 into machine bound updated asset rights 20, and stores 226a the machine-bound updated asset rights 20 within the secure key locker 26, typically over a secure access channel 230.

Burn Operations.

[0077] As seen in Figure 5, the client machine 16 preferably provides burn capabilities 29 of encrypted assets 18 associated with asset rights 20. Upon a user request 209 for a burn 29 of an encrypted asset 18, the digital content player 86 sends 212b a request to the output module 211, which in turn sends a corresponding request 214b to the asset rights module 207, such as over a secure access channel 230, to get the encrypted asset key 22 and encrypted usage rights 24.

[0078] The asset rights module 207 sends a request 216b to the secure key locker 26, such as over a secure access channel 230, to get the machine-bound asset rights

234. In return, the machine-bound asset rights 234 which correspond to the encrypted asset 18 are sent 218b from the secure key locker 26 to the asset rights module 207, preferably over a secure access channel 230. The asset rights module 207 breaks 219 the machine-bound asset rights 234 into the encrypted asset key 22 and encrypted usage rights 24, and sends 220b the encrypted asset key 22 and encrypted usage rights 24 to the output module 211, preferably over a secure access channel 230.

[0079] The output module 211 decrypts the usage rights 24, and determines if the burn 29 is allowed by the usage rights 24. If burn 29 is allowed, the output module 211 decrypts the asset key 22 that is associated with the encrypted asset 18, and decrypts the encrypted asset 18 with the asset key 22, to serve 224b the burn request 212b.

[0080] If the requested burn 29 is not allowed, the output module 211 typically prevents a burn of the asset 18. In some preferred embodiments, the output module 211 may proceed to authorize a playback 27 of a portion or sample of the asset 18, which may be accompanied with a prompt or link to obtain asset rights 20 for the encrypted asset 18.

[0081] If usage rights are affected by burn 29, the output module 211 initiates the required steps to update asset rights 20 into the secure key locker 26. For example, the output module may update and encrypt the asset key 22 and usage rights 24, and send 222b the encrypted updated asset key 22 and usage rights 24 to the asset rights module 207, preferably over a secure access channel 230. The asset rights module 207 binds 217 the encrypted updated asset key 22 to the client machine 16, combines the machine-bound encrypted updated asset key 22 and encrypted updated user rights 24 into machine bound updated asset rights 20, and stores 226a the machine-bound updated asset rights 234 within the secure key locker 26, typically over a secure access channel 230.

Digital Content Player.

[0082] Figure 6 is a functional block diagram 240 of a digital content, *i.e.* media, player 86 associated with a digital music store system 12. A digital content player user interface 242 is linked to the digital content player core 244, which typically comprises digital rights

management 98, a secure digital music store content handler 96, and dedicated communications 100, such as linked to a communications applications 252, for session status and/or change of events. The digital content player core 244 typically handles playback, ripping, playlist management, sign on, sharing with instant messaging, digital rights management, and command line handlers.

[0083] The digital content player core 244 is linked to the operation system and network 260, such as through ODBC/MDB 262 and/or through CD burning SDK 264. A playback engine 250 is also linked to the operation system and network 260, such as to provide functionality for MP3 266, nsv 268, Quicktime™ (QT) 270, secure AAC 272, and/or AAC 274.

[0084] While some elements of the digital content player 86 are specific to operation within the digital content store system 12, other elements, such as the playback engine 250, are preferably shared by one or more music client products, *e.g.* such as for internet radio. As well, some elements may be provided through codec plugins.

Content Intake and Asset Processing.

[0085] Figure 7 is a schematic diagram 300 of content intake 308 , content acquisition and processing 118 and the establishment of an associated asset license 20. A raw asset 304, such as audio, video, game, or multimedia content 304, is typically provided from a source 302, such as from a label 124 (FIG. 2). The raw asset 304 typically comprises associated metadata 306, such as comprising title information, artist information, run time, and/or bonus content. Other metadata 306 associated with the content 304 may be received from the source 302, such as but not limited to pricing, royalty, and/or marketing information, which may or may not be distributed with the content 304.

[0086] The content acquisition and processing 118 comprises asset encoding and encryption 120. In some embodiments of the digital content store system 12, encryption of a received asset 304 comprises NSS encryption or 128-bit AES encryption, such as specified at http://csrc.nist.gov/CryptoToolkit/aes/. An associated asset key 22 is generated for the encrypted asset 18, such as by random generation,

e.g. 128-bit random generation. While the asset key 22 is preferably unique to different encrypted assets 18, the same asset key 22 is preferably used, *i.e.* the key 22 is reused or shared, for content delivered to multiple users USR and/or recipients RCP, which simplifies digital music store operations and provides fast delivery of content 18.

[0087] The encrypted asset 18 file typically also comprises an ETK, DMS, or other file extension, wherein the file comprises an asset/file header, comprising header length, encryption cipher type, and asset metadata, along with the encrypted asset 18.

[0088] The content acquisition and processing module 118 uploads encrypted assets 18 to the download server 110, which acts as content storage 110 (FIG. 2) for the digital content store 14. Some embodiments of the system 12 store asset licenses 20, which comprise asset keys and associated usage rights 24, on the license server 312. As seen in Figure 2, asset keys 22 may be stored in a keys database 114, while content metadata 306 and usage rights 24 is stored separately 112 from the asset keys 22.

[0089] The combined intake, processing, and storage of encrypted assets 18 and associated asset rights 20 provides a secure means to make assets available for licensed purchase and subsequent use through the digital content store 14.

Asset Rights.

[0090] Figure 8 is a functional block diagram of a draft data model 320 within a digital content store system 12. As seen in Figure 8, a user USR may access the digital content store 14 from one or more machines 16.

[0091] For example, a user who is interested in an item, *e.g.* a song 16, that is available from the digital content store 14 can enter purchase information 34 (FIG. 1) from any client machine 16. Use 324 of the content 322, such as an encrypted asset 18, may include any combination of allowed burns 328, or playing 326 of the content from a given machine 14.

[0092] As well, usage of the content 18 may include the controlled specification of one or more machines 16 from which the purchased asset 18 may be associated. For example, while a user may purchase access to a song 18 from a desktop computer 16a, the user may also desire to play the acquired song at a mobile computer 16b, or at

another alternate terminal 16, *e.g.* such as during travel. As well, a user may wish to burn a compact disk CD, such as for personal use or for a gift, either at a primary computer 16 having burn capabilities, or at an alternate terminal 16 that comprises burn capabilities.

Extended Asset Rights.

[0093] The digital music store system 12 provides users USR with an opportunity to go to the content store 14 for single or multiple music tracks. Figure 9 is a schematic diagram 330 of physical content purchase and availability of streamed and/or downloadable content.

[0094] Figure 10 is a functional block diagram of a playlist 340, comprising one or more assets 18a-18k arranged for playback 27, ripping, *i.e.* burning 29, or loading 31. For example, a user USR may selectively arrange different playlists 340, such as to play for work, leisure, parties, commuting, and/or exercise, *e.g.* "Bob's Favorite Gnarly Surf Music".

[0095] Different embodiments of the digital content store system 12 may comprise different usage rights 24 for an acquired asset 18, such as to allow a user to play and/or burn a song 18 or a playlist 340 a set number of times, *e.g.* unlimited playing 27 and ten burns 29, and/or to allow a user USR to play 27 and/or burn 29 a song 18 or playlist 340 on a set number of client machines 16, *e.g.* on three machines 16.

[0096] In the digital music store system 12, a burn limit may apply either to each song 18 individually, or may apply to a playlist 340, which comprises one or more songs 18, as specified by a user USR, to be burned 29 or loaded 31.

Security of Content.

[0097] The digital music system 12 prevents unauthorized use 27, 29, 31 of encrypted assets 18 from client machines 16 which do not have proper authorization. For example, Figure 11 is a schematic diagram 350 of a transfer 352 of an encrypted asset 18, without a proper transfer or extension of asset rights or license 20, from a client machine 16a to a recipient machine 16r. As seen in Figure 11, an attempt 354 to use 27,

29, 31 an encrypted asset 18, without proper asset rights 20, results in a denial of use 356 of the encrypted asset 18.

[0098] Figure 12 is a schematic diagram 360 of a transfer 352 of an encrypted asset 18, with an improper transfer of an associated license 20, from a client machine 16a to a recipient machine 16r. As seen in Figure 12, an attempt 354 to use 27, 29, 31 an encrypted asset 18, with an attempted use 364 of asset rights 20, results in a denial of use 356 of the encrypted asset 18. Therefore, even if an encrypted asset 18 is sent with a "copy" of an associated license, the encrypted asset 18 is still unusable 364, since usage rights 24 are linked to authorized usage 27, 29, and/or 31, such as within a machine 16 having proper ID 21a, *e.g.* machine fingerprinting, or within an authorized transfer 330 (FIG. 9) of the encrypted asset 18 to another machine 16 or device 390, *e.g.* 390a,390b (FIG. 15,FIG. 16)

[0099] Figure 13 is a schematic diagram 370 of a transfer of an encrypted asset 352 and a system prompt 356 to establish authorized use for the encrypted asset 18. In some embodiments of the digital music store system 12, the transfer 352 of an asset without the proper transfer of asset rights 20 does not necessarily result in an absolute denial of use 356. For example, as seen in Figure 13, upon an attempt 354 to use 27, 29, 31 an encrypted asset 18 which lacks proper asset rights 20, a user USR or recipient RCP may be presented with a prompt 374 to access 376 the digital music store 14, such as to purchase the encrypted asset 18 and/or asset rights 20. As well, a sample 372 of the asset 18, *e.g.* such as a sound clip, movie trailer, or game demo sample, may be played for the user USR or recipient RCP, such as provide a teaser or sales incentive to establish proper asset rights 20.

Mixed Media Capabilities and Transfer of Assets or Asset Claims.

[0100] Some embodiments of the digital content store system 12 provide mixed media capability, wherein digital assets 18 and/or physical media 57 may be purchased within the same content store 14. For example, as seen in Figure 1, a user USR may purchase a physical compact disk or DVD 57, which is shipped 58, and/or may purchase digital assets 18, such as a digital album comprised of assets 18.

[0101] As well, in some embodiments of the digital music store system 12, a user USR who purchases physical media 56 may additionally be provided with the ability to stream or download any or all of the album comprised of encrypted assets 18. A user USR can then quickly access and use desired content 18, as specified within associated asset rights 20, while waiting for the physical media 56 to be delivered. The digital rights 20 are controlled by the digital rights management system and a back-end enabling system associated with the digital content store 14.

[0102] Figure 14 is a schematic diagram 380 of a digital music store system 12d, in which a user USR can purchase physical content 57 and or digital content 18 for an alternate recipient RCP, wherein the content is streamed 48 or downloaded 54 to the recipient machine 16b,16n. As well, the purchaser user USR can preferably provide purchase information 382, such as for a monetary amount of physical content 57 and/or digital content 18, wherein the recipient RCP can enter a selection information 384, *e.g.* such as to redeem a gift or allowance toward desired content 57,18.

Digital Content Players.

[0103] Figure 15 is a functional block diagram of a basic digital content player 390. Digital content 18 is typically processed within the client machine 16, and input 392 into the player 390, such as stored 394 as one or more raw digital assets 304a-304n. The device 390 provides playback 395 of one or more songs 18 or playlists 340 (FIG. 10), through device control 393.

[0104] Figure 16 is functional block diagram of a digital music player 400 comprising asset security for encrypted assets 18. Encrypted content 18a-18p is typically transferred from a client machine 16, in compliance with allowed usage rights 24. Some embodiments of the player 400 additionally provide storage and playback of raw, *i.e.* unencrypted assets 304a-304m. As seen in Figure 16, the player 400 typically comprises similar internal digital rights management capabilities, such as a secure key locker 26, and an extended license 20, comprising asset keys 22 and usage rights 24 for the encrypted content 18. The player may typically store one or more device IDs 21, to track the source machine 16 from which content 18 is received. As well, the device

preferably comprises a device ID 410, which is used for machine-bound content management. In some embodiments of the secure content player 400, the player 400 is considered to be a client machine 16, such as for licensing purposes. In alternate embodiments of the secure content player 400, the player 400 is considered to be an independent player, such as for licensed usage allowed for a user USR of one or more client machines 16.

System Advantages.

[0105] The digital content store system 12 and associated methods provide significant advantages over existing content sales and delivery systems. The versatility of the digital content store system 12 readily provides a key entry point for the purchase of content assets 18, such as but not limited to music, video, game, and/or software commerce. For example, in a digital content store system 12 implemented as a digital music store system 12, users USR can search and browse a catalog of downloadable music, such as integrated with a physical goods store 57, providing a physical inventory of music and/or movies.

[0106] Furthermore, some embodiments of the digital content store system 12 allow streaming or download of music and/or video programming, such as to provide internet enabled broadcasting of content, whereby a user USR can readily access and purchase desired content, such as if the listener user likes a song or artist which is played through the digital content player 86.

[0107] The digital content store system 12 provides transparent rights management and commerce-enabled sharing of assets 18. For example, when a user consumes, buys, or shares media, the digital content store system 12 intelligently manages the rights to the media. When a user USR shares and asset 18, the digital content store system 12 preferably enables either the sharer user USR or sharee recipient RCP to purchase rights to the media 18.

[0108] The digital content store system 12 provides a facility through which a user USR can readily browse and purchase usage rights 34 for secure digital assets 18, and prevents casual users from "stealing" assets.

[0109] The digital content store system 12 also provides controlled defined usage, such as to provide basic "counters based" digital rights management, as currently required by labels 124, such as to provide a limited number of burns, as specified by standard Redbook Audio™ standards, or to provide user ownership on a specified number of machines, *e.g.* three machines 16.

[0110] As well, the digital content store system 12 is readily flexible to meet the needs of future digital rights management standards, since there is minimal impact on code, or on purchased assets.

Protection and Rights Management.

[0111] In the digital content store system 12, each raw asset 306 is typically pre-encrypted with a unique, symmetric asset key 22, wherein the asset can only be played using this associated asset key 22. When a user USR purchases an encrypted asset 18, the asset key 22 and usage rights 24 are seamlessly downloaded 54. A license 20, comprising both the usage rights 24 and asset key 22, are preferably downloaded over a secure client/server channel, *e.g.* such as though SSL.

[0112] The user's order and download history 46 are stored on the server, and the user's machine ID (GUID) 21 is stored on the server, as part of the download history 46. The license 20 is bound to the machine 16, such as through "machine fingerprinting", and is stored in the secure key locker 26. As well, client modules that use the licenses 20 and assets 18 are preferably protected using tamper-resistance, *e.g.* such as provided by SAFEWRAP™, by Macrovision, Inc..

[0113] The digital content store system 12 provides a significant music distribution channel, via digital downloads in a secure format. Copy-protection within the digital content store system 12 is a secure yet simple solution. The digital content store system 12 prevents illegal copying of individual songs from one machine 16 to another, while providing legitimate customers with the ability to use their songs 18 in a reasonable manner. As well, the digital content store system 12 enables simple rights management concerning CD burning.

[0114] Although the digital content store system 12 has an understanding of rights management, the system 12 is easy to deploy, and is transparent to the end user. For example, assets 306 are preferably protected using symmetric-key encryption. Once protected, the encrypted assets 18 is safe from all but the most sophisticated attackers, and encrypted assets 18 can be moved around at will by customers. Without the associated asset key 22 for an encrypted asset 18, however, the encrypted asset 18 cannot be played. An asset key 22 is bound to usage rights 24 at the moment of purchase 34, to create a license 20, and valid licenses 20 are only issued by the content store 14. Thus, only customers USR who have purchased valid licenses 20 through the store are able to play back 27 the encrypted asset 18.

[0115] In order to prevent users from being able to move licenses around, each license 20 is bound to a specific machine 16 at the time the license 10 is issued, which prevents users from transferring licenses 20. Machine fingerprinting is preferably used to bind the license 20 to the machine 20, and then the license 20 is stored in a secure key locker 26. Usage information, *e.g.* like the burn count, is also stored in the secure key locker 26. As well, the download module 205, the playback module 211, and the usage rights module 207 are preferably tamper-resistant, such as provided by SAFEWRAP™, by Macrovision, Inc., to deter reverse-engineering.

[0116] In preferred embodiments of the digital content store system 12, content assets 304 are protected by symmetric-key encryption using a secret asset key 22. Each separate asset 304 is protected with a unique asset key 22, but every copy of that asset uses the same asset key 22. Thus, two purchasers USR purchasing the same song 304 receive identically protected assets 18 and identical keys 22. During the content intake process 300 (FIG. 7), incoming assets 304 are preferably encoded into 96-Kbps Dolby AAC, and then encrypted using 128-bit AES in CBC mode. The encrypted encoded assets 18 are then preferably packaged in an ".etk" format, which adds an unencrypted metadata header.

[0117] Once encrypted, these assets 18 are well protected, since without the key 22, AES encryption is very difficult to crack. The digital music store system 12 is designed with knowledge that users commonly try to move and/or distribute content 304,18. Since

encrypted assets 18 can not be played back without an associated key 22, encrypted assets 18 provide no value for unauthorized use or distribution.

[0118] Asset keys 22 can only be obtained through the digital music store 14. Once users have purchased a song, they can download the key on up to N machines, where N is configurable. At present, the default value is three machines. Users USR can also preferably download as many times as they want to the same N machines, in case they accidentally delete the file or their hard drive crashes. Once the user has reached their maximum number of allowed machines, the store does not issue new keys 22, unless the user purchases more licenses 20.

[0119] When a customer purchases an asset 18, that purchase is associated with a predetermined set of usage rights 24, which are combined with the asset key 22 to form a license 20. In some embodiments of the digital music store system 12, usage rights 24 only comprise limits on the number of times a user USR can burn a particular asset to CD. Once on the client machine 16, licenses 20 are bound to the machine 16, such as by machine fingerprinting. Both the licenses and the meter counts (for CD burning) are stored in the secure key locker 26.

[0120] Burning 29 is currently less secure that playing 27, because burning requires that the digital content player 86 write out the asset as an unprotected .wav file, which is currently a limitation of CD burning libraries. Since the burning process 29 necessarily exposes the content in standard Redbook™ CD audio format, there is currently no available alternative. After the burning is considered successful, the burn count stored in the secure key locker 26 is updated to reflect the new count.

System Options.

[0121] Some embodiments of the digital content store system 12 provide a variety of optional benefits for users USR and/or recipients RCPs. For example, the system 12 may preferably provide a free burn count to a complaining user for list of his purchased assets. In such an embodiment, a user USR is typically directed to download this additional burn usage right to the machine 16, such as during the next burn attempt of content 18. As well, the system 12 may preferably provide an additional machine count

to a complaining user, such as in exchange for a list of purchased assets 18. Furthermore, customer can buy additional "licenses" for the same song 18, to extend usage on more machine 16 or players 400. In addition, the system 12 may be readily adapted to provide the same or different usage rights to multiple users USR on a single machine 16. In some system embodiments 12, a customer care server at the digital store 14 preferably allows the user to view download history, whereby user USR provides machine ID 21 to view a download history on a specific machine 16.

[0122] Although the digital content store system and methods of use are described herein primarily in connection with the secure purchase, delivery and playback of music, *i.e.* songs and/or albums, the apparatus and techniques can be implemented for a wide variety of digital content, such as a wide variety of audio content, *e.g.* songs, dialog, discussion, video content, multimedia content, game or video game content, art content, or any combination thereof, as desired.

[0123] Although the digital content store system and methods of use are described herein in connection with personal computers, mobile devices, and other microprocessor-based devices, such as portable digital assistants or network enabled cell phones, the apparatus and techniques can be implemented for a wide variety of electronic devices and systems, or any combination thereof, as desired.

[0124] As well, while the digital content store system and methods of use are described herein in connection with interaction between a client machine and one or more digital content stores across a network, such as the Internet, the digital content store system and methods of use can be implemented for a wide variety of electronic devices and networks or any combination thereof, as desired.

[0125] Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.